EXHIBIT I

Claim 1	RUCKUS DEVICES
A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:	The Ruckus Devices comprise wired access points, routers, and switches that provide Quality of Service ("QoS") support in accordance with the IEEE 802.1p standard. The Ruckus Devices include, but are not limited to the all devices in the ICX 7150 series. The Ruckus Devices perform a method for checking permissibility to use a service. The Ruckus Devices use QoS to check the permissibility of the transmission of a packet stream (e.g., Voice, Video, etc.) in a communications network. 

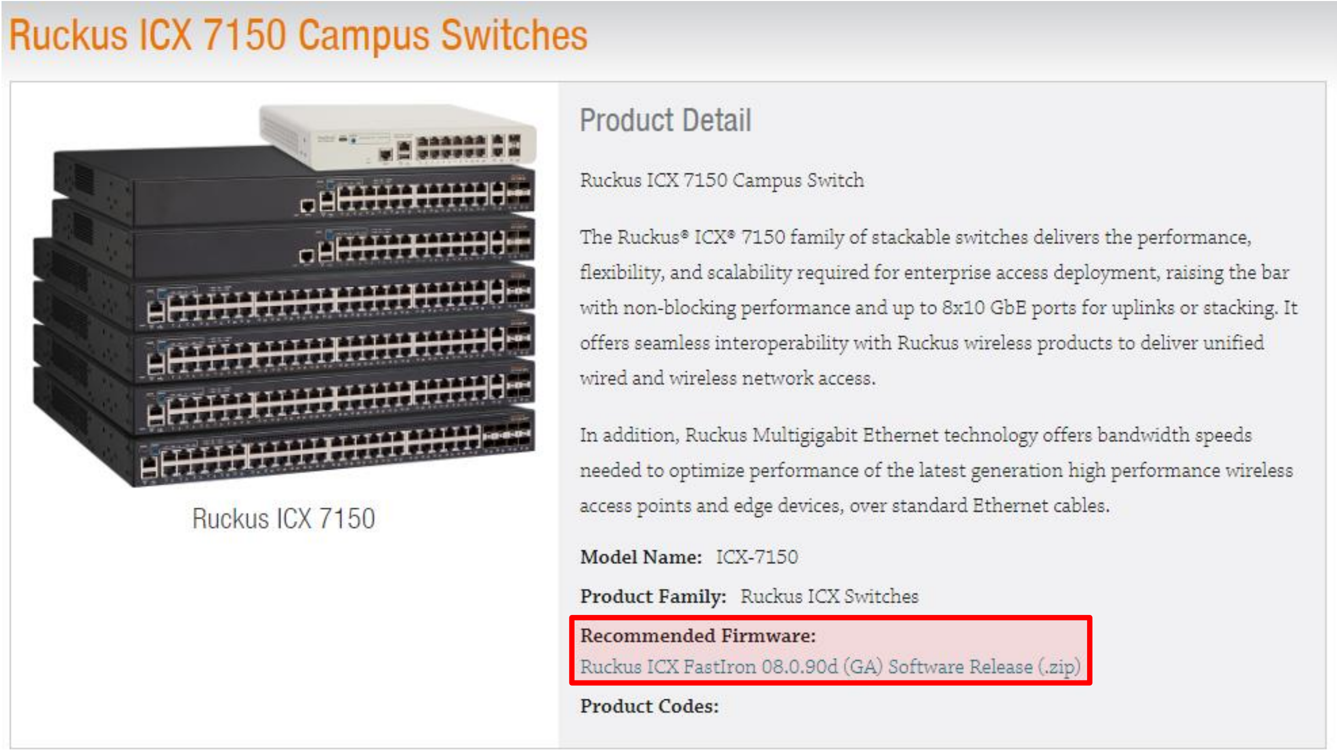
Claim 1	RUCKUS DEVICES
A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:	**The Ruckus Devices comprise wired access points, routers, and switches, including the ICX 7150 series, perform a method for checking permissibility to use a service. The Ruckus Devices use QoS to check the permissibility of the transmission of a packet stream (e.g., Voice, Video, etc.) in a communications network.**

QoS priority queues	• 8 per port	
Multicast groups	• 3,072 (Layer 2) • 2,048 (Layer 3)	
Quality of Service (QoS)	• ACL Mapping and Marking of ToS/DSCP (CoS) • ACL Mapping and Marking of 802.1p • ACL Mapping to Priority Queue • Classifying and Limiting Flows Based on TCP Flags • DiffServ Support	• Honoring DSCP and 802.1p (CoS) • MAC Address Mapping to Priority Queue • Priority Queue Management using Weighted Round Robin (WRR), Strict Priority (SP), and a combination of WRR and SP

Source: Ruckus ICX 7150 Data Sheet, p. 9

Feature	STANDARD COMPLIANCE	
IEEE standards compliance	• 802.1AB LLDP/ LLDP-MED • 802.1D MAC Bridging • 802.1p Mapping to Priority Queue • 802.1s Multiple Spanning Tree (MST) • 802.1w Rapid Reconfiguration of Spanning Tree (RSTP) • 802.1x Port-based Network Access Control (PNAC) • 802.3 Carrier Sense Multiple Access/Collision Detection (CSMA/CD) • 802.3ab 1000BASE-T • 802.3 10Base-T • 802.3ad Link Aggregation (Dynamic and Static) • 802.1 AX-2008 Link Aggregation	• 802.3ae 10 Gigabit Ethernet • 802.3af Power over Ethernet • 802.3at Power over Ethernet Plus • 802.3bz Multigigabit Ethernet • 802.3u 100Base-TX • 802.3x Flow Control • 802.3z 1000Base-SX/LX • 802.3 MAU MIB (RFC 2239) • 802.1Q VLAN Tagging • 802.1BR Bridge Port Extension • 802.3az Energy Efficient Ethernet
RFC standards compliance	For a complete list of RFCs supported by the ICX 7000 product family, please visit www.ruckusnetworks.com/support.	

Source: Ruckus ICX 7150 Data Sheet, p. 10

Claim 1	RUCKUS DEVICES
A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:	 **Source: https://support.ruckuswireless.com/products/108-ruckus-icx-7150-campus-switches#sort=relevancy&f:@commonproducts=[ICX%207150]**

Claim 1	RUCKUS DEVICES
A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:	**The Ruckus Devices implement the service (e.g. VoIP, Video, etc.) in at least one communications network (e.g., the ethernet network).** DATA SHEET COMMSCOPE® Ruckus ICX 7150 Enterprise-Class Stackable Access Switch Entry-Level Access Switch Series Delivers Unprecedented Performance and Features in Its Class The Ruckus® ICX® 7150 series of stackable switches delivers the performance, flexibility, and scalability required for enterprise access deployment, raising the bar with non-blocking performance and up to 8x10 GbE ports for uplinks or stacking. It offers seamless interoperability with Ruckus wireless products to deliver unified wired and wireless network access. In addition, Ruckus Multigigabit Ethernet technology offers bandwidth speeds needed to optimize performance of the latest generation high performance wireless access points and edge devices, over standard Ethernet cables.  **Source: Ruckus ICX 7150 Data Sheet, p. 1**

Claim 1	RUCKUS DEVICES
A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:	**Stacking Across the ICX 7150 Series** Ruckus stacking technology makes it possible to stack up to twelve Ruckus ICX 7150 switches into a single logical switch. This allows the Ruckus ICX 7150 to deliver a class-leading 480 Gbps of aggregated stacking bandwidth and offer simple and robust expandability for future growth. Stacking is supported across the ICX 7150 series and all ICX 7150 models including the ICX 7150 compact switches and the ICX 7150-48ZP can be mixed within the same stack. This stacked switch has only a single IP address that simplifies management and offers transparent forwarding across up to 600×1 GbE ports or up to 192×2.5 GbE ports, and up to 96×10 GbE ports. When new switches join the stack, they automatically inherit the stack's existing configuration file, enabling a plug-and-play network expansion. **Source: Ruckus ICX 7150 Data Sheet, p. 2**

Claim 1	RUCKUS DEVICES
A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:	**Multigigabit Ethernet Support** The Ruckus ICX® 7150-48ZP Switch raises the bar for entry-level switches even further with 16x IEEE 802.3bz compliant 2.5 GbE ports, up to 8x10 GbE uplink ports, dual redundant load sharing power supplies and class-leading stacking density with up to 12 switches per stack. The ICX 7150-C10ZP delivers multigigabit speeds in a compact form factor with support for 2.5/5 and 10 Gbps. Both switches stack with all other members of the ICX 7150 series allowing organizations to buy what they need now and easily scale as the need for Multigigabit support emerges. It is designed to work seamlessly with Ruckus wireless access points to deliver unified wired and wireless network access. **Source: Ruckus ICX 7150 Data Sheet, p. 3**

Claim 1	RUCKUS DEVICES
A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:	Enterprise-Class Features Across Ruckus ICX Switches The Ruckus ICX switch family delivers the enterprise class features for flexibility, scalability and simplified management. • Ruckus Campus Fabric* technology delivers unmatched flexibility, scalability and simplified management for campus network deployments. Incorporating all of the ICX 7000 switch families with up to 1800 ports in a single logical domain, Campus Fabric allows customers the benefits of a traditional chassis, with the flexibility of stackable switches at a dramatically reduced Total Cost of Ownership (TCO). • Advanced stacking* goes beyond traditional stacking with capabilities that take flexibility, ease of management and cost effectiveness to then next level, including: – Stacking on standard Ethernet ports – Long-distance stacking – No hardware module required for stacking – In Service Software Upgrade (ISSU) to minimize downtime – Superior scalability with the industry-leading number of switches per stack – Stacking at the access, aggregation and core layers • Enterprise-Class Availability to improve resiliency and minimize downtime, including: – Hitless stack failover – Hot-insertion/removal of stack members – Redundant power supplies – In Service Software Upgrades for switch stacks • Ruckus offers a broad range of unified management solutions for organizations of all types and sizes: – Ruckus SmartZone network controllers deliver the scale, flexibility to support the most sophisticated deployment scenarios. – Ruckus Cloud eliminates on-premises controllers and management software, moving network management to the cloud. – Ruckus Unleashed is a simple-to-setup, easy-to-run management solution in a package designed for small businesses. • On-boarding and security policies across ICX switches and wireless networks • OpenFlow 1.3 protocol* support in hybrid mode allows user to deploy traditional Layer 2/3 forwarding with OpenFlow on the same port for Software Defined Network (SDN) enabled programmatic control of the network • Open Standards based management, monitoring and authentication – sFlow-based network monitoring to help analyze traffic statistics and trends on every link and overcome unexpected network congestion – Open-standards management includes Command Line Interface (CLI), Secure Shell (SSHv2), Secure Copy (SCP), and SNMPv3 – Support for Access Controller Access Control System (TACACS/TACACS+) and RADIUS authentication helps ensure secure operator access – LLDP and LLDP-MED protocol support for configuring, discovering, and managing network infrastructure such as QoS, security policies, VLAN assignments, PoE power levels, and service priorities **Source: Ruckus ICX 7150 Data Sheet, p. 6**

Claim 1	RUCKUS DEVICES
A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:	**The communications network provided by the Ruckus Devices has an overall transmission capacity. For example, the capacity of the ethernet network.** The following external parameters are associated with each queue that supports the operation of the credit-based shaper algorithm: c) ***portTransmitRate.*** The transmission rate, in bits per second, that the underlying MAC Service that supports transmission through the Port provides. The value of this parameter is determined by the operation of the MAC. d) *idleSlope*. The rate of change of *credit*, in bits per second, when the value of *credit* is increasing (i.e., while *transmit* is FALSE and the transmission gate for the queue is open [8.6.8.4]). The value of *idleSlope* can never exceed *portTransmitRate*. If the enhancements for scheduled traffic (8.6.8.4) are not supported, or if GateEnabled is FALSE (8.6.9.4.14), the value of *idleSlope* for a given queue is equal to the value of the *operIdleSlope(N)* parameter for that queue, as defined in 34.3. If the enhancements for scheduled traffic (8.6.8.4) are supported, and GateEnabled is TRUE (8.6.9.4.14), then *idleSlope* = (*operIdleSlope(N)* × OperCycleTime / GateOpenTime) where OperCycleTime is as defined in 8.6.9.4.20 and GateOpenTime is equal to the total amount of time during the gating cycle that the gate state for the queue is Open. **34.3 The bandwidth availability parameters** The following bandwidth availability parameters exist for each Port, and for each traffic class, N, that supports the credit-based shaper algorithm: a) ***portTransmitRate*** as defined in 8.6.8.2; b) ***deltaBandwidth(N)***: The additional bandwidth, represented as a percentage of *portTransmitRate*, that can be reserved for use by the queue associated with traffic class N, in addition to the *deltaBandwidth(N)* values associated with higher priority queues. For a given traffic class N, the total bandwidth that can be reserved is the sum of the *deltaBandwidth* values for traffic class N and all higher traffic classes, minus any bandwidth reserved by higher traffic classes that support the credit-based shaper algorithm (see 34.3.1). c) ***adminIdleSlope(N)***: The bandwidth, in bits per second, that has been requested by management to be reserved for use by the queue associated with traffic class N. If SRP is in operation, this parameter has no effect; if SRP is not in operation, then the value of *operIdleSlope(N)* is always equal to the value of *adminIdleSlope(N)*. d) ***operIdleSlope(N)***: The actual bandwidth, in bits per second, that is currently reserved for use by the queue associated with traffic class N. This value is used by the credit-based shaper algorithm (8.6.8.2) as the *idleSlope* for the corresponding queue. **Source: https://standards.ieee.org/standard/802_1Q-2018.html**

Claim 1	RUCKUS DEVICES

A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:

The use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network. The Ruckus Devices transmit at least one service-specific traffic stream, for example the traffic stream related to voice/video/background etc. The traffic stream is assigned to the service by the Ruckus Device. The Ruckus Device is assigned to service the ethernet network.

Transmissions include a traffic category. MAC entities determine the priority value associated with MSDUs that belong to a particular traffic category by using the value provided with the MSDU at the MAC service access point.

I.4 Traffic types and priority values

Table I-2 shows the correspondence between traffic types and priority values used to select the defaults in Table 8-5. The default priority used for transmission by end stations is 0. Changing this default would result in confusion and likely in interoperability problems. At the same time, the default traffic type is definitely Best Effort. 0 is thus used both for default priority and for Best Effort, and Background is associated with a priority value of 1. This means that the value 1 effectively communicates a lower priority than 0.

Table I-2—Traffic type acronyms

Priority	Acronym	Traffic type
1	BK	Background
0 (Default)	BE	Best Effort
2	EE	Excellent Effort
3	CA	Critical Applications
4	VI	"Video," < 100 ms latency and jitter
5	VO	"Voice," < 10 ms latency and jitter
6	IC	Internetwork Control
7	NC	Network Control

Source: https://standards.ieee.org/standard/802_1Q-2018.html

Claim 1	RUCKUS DEVICES
A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:	**I.1 Traffic types** A full description of the QoS needs of applications and network services is too complex to be represented by a simple number 0 through 7. The pragmatic aim of traffic classification is to simplify requirements to preserve the high-speed, low-cost characteristics of Bridges. At the margin, potential bandwidth efficiency is traded for simplicity and higher speed operation—historically a good decision in the LAN. The following list of traffic types, each of which can benefit from simple segregation from the others, are of general interest: a) Network Control—characterized by a guaranteed delivery requirement to support configuration an maintenance of the network infrastructure. b) Internetwork Control—in large networks comprising separate administrative domains there is typically a requirement to distinguish traffic supporting the network as a concatenation of those domains from the Network Control of the immediate domain. c) Voice—characterized by less than 10 ms delay and, hence, maximum jitter (one way transmission through the LAN infrastructure of a single campus). d) Video—characterized by less than 100 ms delay, or other applications with low latency as the primary QoS requirement. e) Critical Applications—characterized by having a guaranteed minimum bandwidth as their primary QoS requirement and subject to some form of admission control to ensure that one system or application does not consume bandwidth at the expense of others. The admission control mechanism can range from preplanning of the network requirement at one extreme to bandwidth reservation per flow at the time the flow is started at the other. f) Excellent Effort—or "CEO's best effort," the best-effort type services that an information services organization would deliver to its most important customers. g) Best Effort—for default use by unprioritized applications with fairness only regulated by the effects of TCP's dynamic windowing and retransmission strategy. h) Background—bulk transfers and other activities that are permitted on the network but that should not impact the use of the network by other users and applications. **Source: https://standards.ieee.org/standard/802_1Q-2018.html** 6.5.9 Priority The MAC Service includes priority as a QoS parameter. MA_UNITDATA.request primitives with a high priority may be given precedence over other request primitives made at the same station, or at other stations attached to the same LAN and can give rise to earlier MA_UNITDATA.indication primitives. **Source: https://standards.ieee.org/standard/802_1Q-2018.html**

Claim 1	RUCKUS DEVICES
A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:	**35. Stream Reservation Protocol (SRP)** SRP utilizes three signaling protocols, MMRP (10.9), MVRP (Clause 11) and MSRP (35.1), to establish stream reservations across a bridged network. Within SRP the Multiple MAC Registration Protocol (MMRP) is optionally used to control the propagation of Talker registrations throughout the bridged network (35.2.4.3.1). The Multiple VLAN Registration Protocol (MVRP) is used by end stations and Bridges to declare membership in a VLAN where a Stream is being sourced. This allows the Data Frame Priority (35.2.2.8.5(a)) to be propagated along the path from Talker to Listener(s) in tagged frames. MSRP will not allow Streams to be established across Bridge Ports that are members of the untagged set (8.8.10) for the related VID. The Multiple Stream Registration Protocol (MSRP) is a signaling protocol that provides end stations with the ability to reserve network resources that will guarantee the transmission and reception of data streams across a network with the requested QoS. These end stations are referred to as Talkers (devices that produce data streams) and Listeners (devices that consume data streams). **Source: https://standards.ieee.org/standard/802_1Q-2018.html**

Claim 1	RUCKUS DEVICES
A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:	**35.1 Multiple Stream Registration Protocol (MSRP)** MSRP supports the reservation of resources for streams, each destined for one or more Listeners, and each from a single source, across a bridged network. Transmitted data that conforms to a successful stream reservation will not be discarded by any Bridge due to congestion on a LAN. In order to propagate requests for reservations, MSRP defines an *MRP application* that provides the Stream resource registration service defined in 35.2.3. MSRP makes use of the MRP Attribute Declaration (MAD) function, which provides the common state machine descriptions defined for use in MRP-based applications. The MRP architecture, and MAD are defined in Clause 10. MSRP defines a new MRP Attribute Propagation (MAP) function, to provide an attribute propagation mechanism. MSRP propagates registrations for stream reservations in a manner similar to the operation of MMRP (10.9) and MVRP (11.2), which are used for registering Group membership and individual MAC address information, and VLAN membership, respectively. Unlike MMRP and MVRP, however, the registered attributes can be combined, discarded, or otherwise altered, as they are propagated by the participating Bridges. In order to make and keep QoS guarantees all devices in a bridged network must participate in the signaling and queuing operations required of Bridges. For example, this would include IEEE 802.11 wireless media access points and stations. Thus, MSRP provides a means for Bridges or end stations running MSRP to cooperate both with higher network layers, such as routers or hosts running RSVP, and with lower network layers, such as wireless media. **Source: https://standards.ieee.org/standard/802_1Q-2018.html**

Claim 1	RUCKUS DEVICES
analyzing the use of the service with an access control function which is assigned to the access node; and	The Ruckus Devices analyze the use of the service with an access control function which is assigned to the access node. The Ruckus Devices analyze the service (e.g., voice/video/background) with an access control function (e.g., a function that results from a SRP registration) that is assigned to the access node. The function results in analysis of the traffic specification for the stream, which defines the MaxFrameSize of the MSDU and the MaxIntervalFrames. 34.2 Detection of SRP domains The concept of audio/video (AV) streams, the Stream Reservation Protocol (SRP), and the traffic forwarding and shaping functions that support stream transmission (see 6.9.4 and 8.6.8.1), rely on the ability of each Bridge to detect whether each of its ports is at the edge of a region of connected Bridges that support SRP on a particular priority, so that the Priority Code Point values associated with traffic entering an *SRP domain* (3.257) can be properly regenerated at the boundary of the domain, as described in 6.9.4. Bridges detect the edge of an SRP domain by observing SRP behavior. If a Bridge receives SRP registrations using a particular priority, then it is reasonable to believe that they are being received from an SRP-capable device; the SRP engine can therefore signal which Ports of a Bridge are at the boundary of an SRP domain. The per-port, per-SR class, *SRPdomainBoundaryPort* parameter determines whether a Port is considered to be at the edge of an SRP domain or within the core of the domain, as defined in 35.1.4. This parameter is controlled by the operation of SRP. Source: https://standards.ieee.org/standard/802_1Q-2018.html

Claim 1	RUCKUS DEVICES
analyzing the use of the service with an access control function which is assigned to the access node; and	**34. Forwarding and Queuing Enhancements for time-sensitive streams (FQTSS)** 34.1 Overview This clause describes a set of tools that can be used to support the forwarding and queuing requirements of time-sensitive streams. In this context, a "time-sensitive stream" is taken to be a stream of traffic, transmitted from a single source station, destined for one or more destination stations, where the traffic is sensitive to timely delivery, and in particular, requires transmission latency to be bounded. Such streams include video or audio data streams, where there is a desire to limit the amount of buffering required in the receiving station. NOTE 1—An example of this requirement would be a live performance where a video image of the performance is simultaneously projected on a screen in the auditorium, and it is desirable for the sound and image to be "in sync" with the performance. In order to address the needs of such traffic in Bridges, the following are provided: a) A means of detecting the boundary between a set of Bridges that support SRP (an SRP domain) and surrounding Bridges that do not support SRP. This mechanism is described in 34.2. NOTE 2—The primary intent of these functions is to support SRP; however, there is no specific interdependency between these functions and SRP, so they could equally be used to support other admission control mechanisms if they were implemented. b) A set of bandwidth availability parameters for each port that are used to record the maximum bandwidth available to a given outbound queue, and the actual bandwidth reserved, for that queue. These parameters are described in 34.3. c) A credit-based shaper algorithm, defined in 8.6.8.1, that is used to shape the transmission of stream-based traffic in accordance with the bandwidth that has been reserved on a given outbound queue. d) A discussion of the relationship between the size of the layer 2 "payload" (the MSDU) carried in a frame and how that relates to the actual bandwidth that will be consumed when that MSDU is transmitted on a particular Port (34.4). e) An algorithm for determining the mapping of the priorities associated with received frames onto the traffic classes available on the transmission Ports of a Bridge (34.5). f) A definition of the required behavior of an end station that acts as the source of a time-sensitive data stream (34.6). **Source: https://standards.ieee.org/standard/802_1Q-2018.html**

Claim 1	RUCKUS DEVICES
analyzing the use of the service with an access control function which is assigned to the access node; and	**34.5 Mapping priorities to traffic classes for time-sensitive streams** In Bridges that support FQTSS, the default mappings of priorities to traffic classes meet the following constraints: a) Priority values that correspond to SR classes are mapped onto traffic classes that support the credit-based shaper algorithm as the transmission selection algorithm. b) Traffic classes that support the credit-based shaper algorithm have a higher priority than traffic classes that support the strict priority (or any other) transmission selection algorithm. c) At least one traffic class supports the credit-based shaper algorithm, and at least one traffic class supports the strict priority transmission selection algorithm. NOTE 1—The constraint that there is at least one traffic class that supports the strict priority transmission selection ensures that there is at least one traffic class that can support traffic that is not subject to bandwidth reservation, such as "best effort" traffic. The recommended default priority to traffic class mappings for a system that supports SR class A (using priority 3) and SR class B (using priority 2) are shown in Table 34-1. The recommended default priority to traffic class mappings for a system that supports only SR class B (using priority 2) are shown in Table 34-2. **Source: https://standards.ieee.org/standard/802_1Q-2018.html**

Claim 1	RUCKUS DEVICES
checking, via the access control function, without further interrogations at internal transmission nodes of the communications network, whether the use of the service is permitted, the checking performed taking into account an available capacity, which is	**The Ruckus Devices practice checking, via the access control function, without further interrogations at internal transmission nodes of the communications network, whether the use of the service (e.g., voice/video/background) is permitted, the checking performed taking into account an available capacity, which is determined taking into account the overall transmission capacity (e.g., bandwidth parameters), and available to the access node for transmitting traffic streams to the communications network. As part of the Stream Reservation Protocol, the Ruckus Devices checks to see if it can reserve the bandwidth and then passes the reservation request on to the next hop in the network.** **34.3 The bandwidth availability parameters** The following bandwidth availability parameters exist for each Port, and for each traffic class, N, that supports the credit-based shaper algorithm: a) *portTransmitRate* as defined in 8.6.8.2; b) *deltaBandwidth(N)*: The additional bandwidth, represented as a percentage of *portTransmitRate*, that can be reserved for use by the queue associated with traffic class N, in addition to the *deltaBandwidth(N)* values associated with higher priority queues. For a given traffic class N, the total bandwidth that can be reserved is the sum of the *deltaBandwidth* values for traffic class N and all higher traffic classes, minus any bandwidth reserved by higher traffic classes that support the credit-based shaper algorithm (see 34.3.1). c) *adminIdleSlope(N)*: The bandwidth, in bits per second, that has been requested by management to be reserved for use by the queue associated with traffic class N. If SRP is in operation, this parameter has no effect; if SRP is not in operation, then the value of *operIdleSlope(N)* is always equal to the value of *adminIdleSlope(N)*. d) *operIdleSlope(N)*: The actual bandwidth, in bits per second, that is currently reserved for use by the queue associated with traffic class N. This value is used by the credit-based shaper algorithm (8.6.8.2) as the *idleSlope* for the corresponding queue. In all cases, bandwidth is defined in terms of the actual bandwidth consumed when frames are transmitted through the Port, not the size of the MSDU "payload" carried within those frames. Subclause 34.4 discusses the relationship between MSDU size and actual bandwidth consumed. NOTE—While the deltaBandwidth values are specified with respect to specific traffic classes, and indicate the amount of bandwidth that can be reserved for traffic belonging to a particular traffic class, this does not imply that these traffic classes have preferential access to that portion of the bandwidth. The priority of a given traffic class does not, for example, imply anything about the importance of a data stream that uses that class; the reservation strategy might therefore allocate bandwidth to a high importance stream that uses a lower priority traffic class in preference to a stream of lower importance that uses a higher priority traffic class. **Source: https://standards.ieee.org/standard/802_1Q-2018.html**

<table>
<tr><th>Claim 1</th><th>RUCKUS DEVICES</th></tr>
<tr><td>checking, via the access control function, without further interrogations at internal transmission nodes of the communications network, whether the use of the service is permitted, the checking performed taking into account an available capacity, which is</td><td>

35. Stream Reservation Protocol (SRP)

SRP utilizes three signaling protocols, MMRP (10.9), MVRP (Clause 11) and MSRP (35.1), to establish stream reservations across a bridged network.

Within SRP the Multiple MAC Registration Protocol (MMRP) is optionally used to control the propagation of Talker registrations throughout the bridged network (35.2.4.3.1).

The Multiple VLAN Registration Protocol (MVRP) is used by end stations and Bridges to declare membership in a VLAN where a Stream is being sourced. This allows the Data Frame Priority (35.2.2.8.5(a)) to be propagated along the path from Talker to Listener(s) in tagged frames. MSRP will not allow Streams to be established across Bridge Ports that are members of the untagged set (8.8.10) for the related VID.

The Multiple Stream Registration Protocol (MSRP) is a signaling protocol that provides end stations with the ability to reserve network resources that will guarantee the transmission and reception of data streams across a network with the requested QoS. These end stations are referred to as Talkers (devices that produce data streams) and Listeners (devices that consume data streams).

35.2.2.8.4 TSpec

The 32-bit TSpec component is the TSpec associated with a Stream. It consists of the following two elements (which are encoded as described in 10.8.1.1):

a) MaxFrameSize: The 16-bit unsigned MaxFrameSize component is used to allocate resources and adjust queue selection parameters in order to supply the QoS requested by an MSRP Talker Declaration. It represents the maximum frame size that the Talker will produce, excluding any overhead for media-specific framing (e.g., preamble, IEEE 802.3 header, Priority/VID tag, CRC, interframe gap). As the Talker or Bridge determines the amount of bandwidth to reserve on the egress port it will calculate the media-specific framing overhead on that port and add it to the number specified in the MaxFrameSize field.
b) MaxIntervalFrames: The 16-bit unsigned MaxIntervalFrames component is used to allocate resources and adjust queue selection parameters in order to supply the QoS requested by an MSRP Talker Declaration. It represents the maximum number of frames that the Talker may transmit in one “class measurement interval” (34.4).

Source: https://standards.ieee.org/standard/802_1Q-2018.html
</td></tr>
</table>

Claim 1	RUCKUS DEVICES
checking, via the access control function, without further interrogations at internal transmission nodes of the communications network, whether the use of the service is permitted, the checking performed taking into account an available capacity, which is	**34.4 Deriving actual bandwidth requirements from the size of the MSDU** The forwarding and queuing mechanisms defined in this clause use bandwidth parameters that are defined in terms of the actual bandwidth used when frames are transmitted on the medium that supports the MAC Service available through the Port. In contrast, the SRP makes use of a traffic specification (TSpec) for each stream that defines the maximum number of bits per frame (*MaxFrameSize*), of the mac_service_data_unit parameter that is relayed by the relay function of the Bridge, and a maximum frame rate (*MaxIntervalFrames*), in frames per class measurement interval, for that stream; i.e., the TSpec takes no account of the per-frame overhead associated with transmitting the MSDU over a given medium. However, when SRP determines the value to be used for the ***operIdleSlope(N)*** parameter associated with a given queue, it is necessary for this value to include the per-frame overhead that will be incurred when frames are transmitted on that Port. NOTE 1—The frame rate in a TSpec is measured over a "class measurement interval" that depends upon the SR class associated with the stream. SR class A corresponds to a class measurement interval of 125 µs; SR class B corresponds to a class measurement interval of 250 µs. These class measurement intervals apply at the source of the stream, i.e., the "Talker" end station, and do not necessarily hold good for subsequent stages in the stream's transmission across a Bridged Network. For the purposes of calculating the bandwidth consumption of a stream, it is assumed that the stream data is essentially of constant size and transmission rate, so these maxima can be used to directly define an assumed maximum payload size and the maximum frame rate in frames per second; i.e., $assumedPayloadSize = MaxFrameSize$ (34-1) $maxFrameRate = MaxIntervalFrames \times (1/classMeasurementInterval)$ (34-2) where *classMeasurementInterval* is measured in seconds. NOTE 2—As stated, the calculation of bandwidth from TSpec parameters assumes that the stream data is essentially of constant frame size, and hence, the approximations shown in this section are valid. If the data varies significantly in frame size, then the calculation of per-frame overhead using these assumptions could be significantly in error. From this, and also from local knowledge of the protocol stack that supports the Bridge Port, it is possible to determine the overhead that is added to the per-frame MSDU payload when a frame is transmitted. There are at least the following sources of per-frame overhead: a) Any VLAN tags and security tags (see IEEE Std 802.1AE) that are added to the layer 2 payload as it passes through the various service interfaces in the Port's protocol stack. b) The MAC framing (header and trailer octets, plus any padding octets that are required to meet minimum frame size limitations) that is added by the underlying MAC Service. c) Any physical layer overhead, such as preamble characters and inter-frame gaps. The precise per-frame overhead will therefore depend upon the protocol stack and the underlying MAC technology. The actual bandwidth needed to support a given stream is therefore defined as follows [using *assumedPayloadSize* from Equation (34-1)]: $actualBandwidth = (perFrameOverhead + assumedPayloadSize) \times maxFrameRate$ (34-3) **Source: https://standards.ieee.org/standard/802_1Q-2018.html**

Claim 1	RUCKUS DEVICES
determined taking into account the overall transmission capacity, and available to the access node for transmitting traffic streams to the communications network.	The available capacity is determined taking into account the overall transmission capacity, and available to the access node for transmitting traffic streams to the communications network. The checking includes determining the bandwidth available, the bandwidth required, and the overall transmission capacity. The "Insufficient bandwidth for traffic class" failure code suggests that the whether the service usage comprising of that particular traffic streams is possible or not and thus is done on the basis of transmission capacity and QOS capacity available. Table 35-6—Reservation Failure Codes (see table below) Source: https://standards.ieee.org/standard/802_1Q-2018.html

Table 35-6—Reservation Failure Codes

Failure Code	Description of cause
1	Insufficient bandwidth
2	Insufficient system resources
3	Insufficient bandwidth for traffic class.
4	StreamID in use by another Talker
5	Stream destination_address already in use
6	Stream preempted by higher rank
7	Reported latency has changed
8	Egress port is not AVB capable[a]
9	Use a different destination_address (i.e., MAC DA hash table full)
10	Out of MSRP resources
11	Out of MMRP resources
12	Cannot store destination_address (i.e., system is out of MAC DA resources)
13	Requested priority is not an SR Class (3.259) priority
14	MaxFrameSize [35.2.2.8.4 item a)] is too large for media
15	msrpMaxFanInPorts [35.2.1.4 item f)] limit has been reached
16	Changes in FirstValue for a registered StreamID.
17	VLAN is blocked on this egress port (Registration Forbidden)[b]
18	VLAN tagging is disabled on this egress port (untagged set)
19	SR class priority mismatch

Claim 1	RUCKUS DEVICES
determined taking into account the overall transmission capacity, and available to the access node for transmitting traffic streams to the communications network.	**34.3.1 Relationships among bandwidth availability parameters** The recommended default value of *deltaBandwidth(N)* for the highest numbered traffic class supported is 75%, and for any lower numbered traffic classes, the recommended default value is 0%. The *deltaBandwidth(N)* for a given *N*, plus the *deltaBandwidth(N)* values for any higher priority queues (larger values of *N*) defines the total percentage of the Port's bandwidth that can be reserved for that queue and all higher priority queues. For the highest priority queue, this means that the maximum value of *operIdleSlope(N)* is *deltaBandwidth(N)*% of *portTransmitRate*. However, if *operIdleSlope(N)* is actually less than this maximum value, any lower priority queue that supports the credit-based shaper algorithm can make use of the reservable bandwidth that is unused by the higher priority queue. So, for queue N-1, the maximum value of (*operIdleSlope(N)* + *operIdleSlope(N-1)*) is (*deltaBandwidth(N)* + *deltaBandwidth(N-1)*)% of *portTransmitRate*. NOTE 1—For example, suppose two queues, 3 and 2, support the credit-based shaper algorithm for SR classes A and B, respectively. Suppose *deltaBandwidth(3)* for SR class A is currently 20%, and *deltaBandwidth(2)* for SR class B is currently 30%. If *operIdleSlope(3)* is currently 10% of *portTransmitRate*, then half of queue 3's maximum allocation is unused, and the maximum value of *operIdleSlope(2)* is therefore currently 40% of *portTransmitRate*. However, if *operIdleSlope(3)* increases to the full 20% that it is entitled to use, the maximum value of *operIdleSlope(2)* reduces to 30% of *portTransmitRate*. NOTE 2—The sum of the *deltaBandwidth(N)* values for all values of N should be chosen such that there is sufficient bandwidth available for any nonreserved (best-effort, strict-priority) traffic; the default values are chosen such that the sum of the *deltaBandwidth(N)* values is 75%, so no more than 75% of the Port's available bandwidth is permitted to be reserved. This ensures that when using default settings, there is at least 25% of the Port's bandwidth available for nonreserved traffic. However, as these default settings may be inappropriate for some situations (e.g., links that offer very high bandwidth, or networks with very low levels of nonreserved traffic), they can be modified by management. **Source: https://standards.ieee.org/standard/802_1Q-2018.html**

Claim 1	RUCKUS DEVICES
determined taking into account the overall transmission capacity, and available to the access node for transmitting traffic streams to the communications network.	**35.2.2.4 MSRP AttributeType definitions** MSRP defines four AttributeTypes (10.8.2.2) that are carried in MRP exchanges. The numeric values for the AttributeType are shown in Table 35-1 and their use is defined by the following list: a) **Talker Advertise Vector Attribute Type:** Attributes identified by the Talker Advertise Vector Attribute Type are instances of VectorAttributes (10.8.1), used to identify a sequence of values of Talker advertisements for related Streams that have not been constrained by insufficient bandwidth or resources. b) **Talker Failed Vector Attribute Type:** Attributes identified by the Talker Failed Vector Attribute Type are instances of VectorAttributes, used to identify a sequence of values of Talker advertisements for related Streams that have been constrained by insufficient bandwidth or resources. c) **Listener Vector Attribute Type:** Attributes identified by the Listener Vector Attribute Type are instances of VectorAttributes, used to identify a sequence of values of Listener requests for related Streams regardless of bandwidth constraints. Listener Vector Attribute Types are subdivided into individual Declaration Types via the MSRP FourPackedEvents (35.2.2.7.2). d) **Domain Vector Attribute Type:** Attributes identified by the Domain Vector Attribute Type are instances of VectorAttributes, used to identify a sequence of values that describe the characteristics of an SR class. **Source: https://standards.ieee.org/standard/802_1Q-2018.html**